Deutscher Bundestag **Drucksache 19/11920**

19. Wahlperiode 25.07.2019

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Tobias Pflüger, Andrej Hunko, Michel Brandt, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 19/11330 –

Rechtlich-organisatorischer Rahmen militärischer Cyber-Operationen

Vorbemerkung der Bundesregierung

Im Jahr 2017 wurden verschiedene Dienststellen der Bundeswehr im Kommando Cyber- und Informationsraum (KdoCIR) zusammengelegt und mit dem Aufbau operativer Fähigkeiten begonnen (https://bit.ly/2Qj0wJ9). Das CERT (Computer-Emergency-Response-Team) der Bundeswehr (CERTBw) war bis dahin als defensive Einrichtung zum Schutz der IT-Netze der Bundeswehr bis zur Gründung des KdoCIR dem IT-Amt der Bundeswehr unterstellt und von der Gruppe Computer Netzwerk Operationen (CNO) im Kommando Strategische Aufklärung (KSA) getrennt. Mit der Aufstellung des KdoCIR wurden CERTBw und CNO den beiden neuen Dienststellen Zentrum Cyber-Operationen und Zentrum für Cyber-Sicherheit der Bundeswehr zugewiesen (https://bit.ly/2QwUGUQ). Das CERTBw hat bisher am CERT-Verbund mit Unternehmen, wissenschaftlichen Organisationen und zivilen Behörden teilgenommen und konnte sich so der Kompetenz und Erfahrung ziviler Akteure bedienen (www.cert-verbund.de/).

Während für den Schutz der Sicherheit und Vertraulichkeit von IT-Systemen nur mäßige Aufwüchse zu erkennen sind, baut die Bundesregierung im Bereich des Militärs und der Geheimdienste mit erheblichen finanziellen und personellen Ressourcen Strukturen auf, die aus Sicht der Fragestellerinnen und Fragesteller nicht mehr allein den Schutz vor bzw. die Abwehr von Cyberangriffen zur Aufgabe haben.

So wird von Vertretern der Bundesregierung und einschlägiger Stellen diskutiert, offensive Cyber-Operationen – sogenannte Hackbacks – in den Aufgabenkatalog aufzunehmen (z. B. hier: http://gleft.de/2Wo). Mit diesen offensiven Cyber-Operationen sind Eingriffe in Computersysteme in anderen Staaten gemeint, die aus Sicht der Fragestellerinnen und Fragesteller den Verpflichtungen aus internationalen Abkommen zuwider laufen und erhebliche sicherheitspolitische und militärische Risiken verursachen. Ein vom NATO Cooperative Cyber Defence Centre of Excellence berufenes Expertengremium hat im sog. Tallinn-Handbuch in einer Bewertung internationalen Rechts formuliert, dass Cyber-Angriffe, die von einem Staatsgebiet ausgehen und nicht unterbunden werden, einen Bruch internationalen Rechts darstellen (https://ccdcoe.org/research/tallinn-manual/). Werden diese von staatlichen Stellen verübt, können

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums der Verteidigung vom 24. Juli 2019 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

sie als Kriegshandlungen gewertet werden, die dem angegriffenen Staat die Rechtfertigung geben, gleichwertige Gegenmaßnahmen zu ergreifen – bei schweren Schäden auch in Form militärischer Aktionen (http://csef.ru/media/articles/3990/3990.pdf).

Die US-Administration hat in ihrer im September 2018 vorgelegten „National Cyber Strategy" angekündigt, eine internationale Cyber-Abschreckungs-Initiative zu verfolgen und dafür gleichgesinnte Staaten in eine gemeinsame Abwehrstrategie einzubinden (vgl. https://bit.ly/2xrQ0XK).

Im Aachener Vertrag einigten sich die Bundesrepublik Deutschland und Frankreich auf die Zusammenarbeit im Bereich der Forschung und des digitalen Wandels, einschließlich der Themen Künstliche Intelligenz und Sprunginnovationen (vgl. Aachener Vertrag, Artikel 21, https://bit.ly/2IM1Lxf).

Vorbemerkung der Bundesregierung

Der von den Fragestellern verwendete Begriff „Hackback" wird von der Bundesregierung konzeptionell grundsätzlich nicht verwendet, weder für Aktivitäten der Cyber-Abwehr noch der Cyber-Verteidigung. Der Beantwortung dieser Kleinen Anfrage legt die Bundesregierung die Begrifflichkeiten aus der Vorbemerkung der Bundesregierung in der Antwort auf die Kleine Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/2645 zugrunde.

Die Behauptung der Fragesteller, für den Schutz der Sicherheit und Vertraulichkeit von IT-Systemen seien nur mäßige Aufwüchse personeller und finanzieller Art zu erkennen, wird von der Bundesregierung zurückgewiesen. Allein der Stellenhaushalt des Bundesamtes für die Sicherheit in der Informationstechnik (BSI), das nach § 1 Satz 2 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) für die Informations-sicherheit auf nationaler Ebene zuständig ist, wuchs mit den Haushalten 2018/2019 um mehr als 50 Prozent auf. Für das Haushaltsjahr 2020 setzt sich die Bundesregierung für einen weiteren Stellenaufwuchs ein.

1. Kann die Bundesregierung Presseberichte bestätigen, wonach die meisten weltweiten Cyberangriffe im Jahr 2018 von Servern in den USA ausgingen und an zweiter Stelle die Niederlande und an dritter Stelle Deutschland stehen (http://gleft.de/2Wr)?

Die Beantwortung dieser Frage als Verschlusssache (VS) mit dem Geheimhaltungsgrad „VS – Nur für den Dienstgebrauch" wird im Hinblick auf das Staatswohl als erforderlich erachtet, da die offene Bekanntgabe Informationen zur Kooperation mit ausländischen Nachrichtendiensten und Methoden des Bundesnachrichtendienstes einem nicht eingrenzbaren Personenkreis nicht nur im Inland, sondern auch im Ausland zugänglich machen würde. Zudem können sich Nachteile für die zukünftige Zusammenarbeit mit ausländischen Nachrichtendiensten ergeben. Dies kann für die wirksame Erfüllung der gesetzlichen Aufgaben der Nachrichtendienste und damit für die Interessen der Bundesrepublik Deutschland nachteilig sein.

Auf die eingestufte Anlage wird verwiesen.*

Darüber hinaus führt die Bundesregierung keine Statistiken im Sinne der Anfrage.

* Das Bundesministerium der Verteidigung hat die Antwort als „VS – Nur für den Dienstgebrauch" eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

2. Falls die Bundesregierung von anderen Zahlen ausgeht, auf welche Quellen stützt sie sich dabei?

Hinsichtlich der Einstufung als Verschlusssache mit dem Geheimhaltungsgrad „VS – Nur für den Dienstgebrauch“ und der Beantwortung wird auf die Antwort zu Frage 1 verwiesen.*

Darüber hinaus liegen der Bundesregierung diesbezüglich keine über die öffentlich zugänglichen Informationen hinausgehenden Erkenntnisse vor.

3. Was kann die Bundesregierung zum aktuellen Stand ihrer Überlegungen für eine „aktive Cyber-Abwehr“ mitteilen („Seehofer plant den Gegenangriff“, www.tagesschau.de vom 29. Mai 2019), und inwiefern betreffen diese auch die Bundeswehr und deren Kommando Cyber- und Informationsraum (KdoCIR)?

4. Inwiefern erwägt die Bundesregierung Hackbacks auch bei Angriffen, die von Systemen traditioneller Geheimdienste ausgehen?

5. Inwiefern erwägt die Bundesregierung Hackbacks auch bei Angriffen, die von Systemen befreundeter Geheimdienste ausgehen?

Wegen des Sachzusammenhangs werden die Fragen 3 bis 5 gemeinsam beantwortet.

Die im Zusammenhang mit Maßnahmen der aktiven Cyber-Abwehr aufgeworfenen Fragestellungen werden derzeit von der Bundesregierung geprüft. Diese Prüfungen sind noch nicht abgeschlossen.

6. Inwiefern wäre ein Hackback durch deutsche militärische Stellen aus Sicht der Bundesregierung von der Budapest Convention on Cybercrime gedeckt, bzw. welche Änderungen wären diesbezüglich erforderlich?

Zur Beantwortung wird auf die Vorbemerkung der Bundesregierung und die Antwort zu Frage 1 der Kleinen Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/2645 sowie auf die Vorbemerkung der Bundesregierung zur Antwort auf die Kleine Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/5472 verwiesen. Des Weiteren wird auf die Antwort der Bundesregierung zu Frage 8 der Kleinen Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN auf Bundestagsdrucksache 19/3420 verwiesen.

7. Inwiefern war die Bundesregierung bezüglich einer internationalen Cyber-Abschreckungs-Initiative bereits in Kontakt mit US-Stellen, und unter welchen Rahmenbedingungen würde sie sich an einer solchen Initiative beteiligen?

Die Bundesregierung ist kontinuierlich bemüht, die eigene Resilienz und Cyberabwehrfähigkeit zu erhöhen, und steht dazu im Kontakt mit einer Vielzahl von Staaten, darunter den USA. Die Erhöhung der eigenen Resilienz kann unter Umständen auch eine abschreckende Wirkung entfalten. Die Bundesregierung ist bemüht, das eigene Vorgehen mit dem Vorgehen wichtiger Partner – vor allem auf europäischer Ebene – zu koordinieren. Der Bundesregierung ist bekannt, dass eine internationale Cyberabschreckungsinitiative Teil der im September 2018 angenommenen „Nationalen Cyberstrategie der Vereinigten Staaten von Amerika“

* Das Bundesministerium der Verteidigung hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

ist. Nach Kenntnisstand der Bundesregierung wird dabei aber keine Beteiligung anderer Länder angestrebt, die über die oben beschriebene Koordinierung hinausgeht.

8. In welchen Formaten hat sich die Bundesregierung an internationalen Gesprächsrunden, Verhandlungen oder Gremien

   a) zum Thema Cybersicherheit allgemein seit 2011 beteiligt (bitte nach Ressorts aufschlüsseln),

Bundeskanzleramt:

- Formate der unter deutscher Schirmherrschaft durchgeführten Münchner Sicherheitskonferenz
- Potsdamer Konferenz für Nationale Cybersicherheit

Auswärtiges Amt:

- NATO Cyber Defence Committee
- Gruppe der Regierungssachverständigen der Vereinten Nationen zum Thema internationale Cybersicherheit (GGE) 2012 – 2013, 2014 – 2015 sowie, unter deutschem Vorsitz, 2016 – 2017
- Horizontale Ratsarbeitsarbeitsgruppe der Europäischen Union zu „Fragen des Cyberraums“ sowie deren Vorgängerformation „Gruppe der Freunde der Ratspräsidentschaft zu Cyberfragen“
- Informelle Arbeitsgruppe Informations- und Kommunikationstechnologie der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE)
- „Freedom Online Coalition“, eine informelle Koalition von 30 Staaten aus fünf Kontinenten, die sich außenpolitisch für Menschenrechte im Internet einsetzt
- Wassenaar-Arrangement für die Exportkontrolle konventioneller Rüstungsgüter und Güter mit doppeltem Verwendungszweck (Dual-Use Güter) und von Technologie in Bezug auf Genehmigungspflichten für den Export bestimmter Schadsoftware (Wahrnehmung gemeinsam mit BMWi).
- Anlassbezogene multilaterale oder bilaterale Gespräche zum Thema Cybersicherheit

Bundesministerium des Innern, für Bau und Heimat:

- Horizontale Ratsarbeitsgruppe der Europäischen Union zu Cybersicherheitsangelegenheiten „Fragen des Cyberraums“ sowie deren Vorgängerformation „Gruppe der Freunde der Ratspräsidentschaft zu Cyberfragen“
- Kooperationsgruppe nach Artikel 11 der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union
- GGE der Vereinten Nationen zum Thema internationale Cybersicherheit (unter Federführung des Auswärtigen Amts)
- Regelmäßiger Austausch mit strategisch wichtigen Partnern innerhalb und außerhalb der EU zu übergeordneten Fragen der Cybersicherheitspolitik

Bundesministerium der Verteidigung:

- Capability Panel Information Assurance and Cyber Defense der Substruktur des Command and Control Consultation Board der NATO
- Steering Committee des NATO Cooperative Cyber Defence Centre of Excellence
- Bilaterale Dialoge im Rahmen des bilateralen Jahresprogramms des Bundesministeriums der Verteidigung sowie mit NATO- und EU-Partnern
- GGE der Vereinten Nationen zum Thema internationale Cybersicherheit (unter Federführung des Auswärtigen Amts)
- Informelle Arbeitsgruppe Informations- und Kommunikationstechnologie der Organisation für Sicherheit und Zusammenarbeit in Europa (unter Federführung des Auswärtigen Amts)

Bundesministerium der Finanzen:

- Horizontale Ratsarbeitsgruppe der Europäischen Union zu Cybersicherheitsangelegenheiten „Fragen des Cyberraums“ sowie in deren Vorgängerformation „Gruppe der Freunde der Ratspräsidentschaft zu Cyberfragen“
- G7 Cyber Experts Group
- G7 Cross Border Coordination Exercise Working Group
- Financial Stability Board: Cyber Lexicon Working Group
- Regelmäßiger bilateraler Austausch zu Cyberthemen im Finanzsektor mit einzelnen EU-Staaten, USA und Israel

b) zu Fragen der Abrüstung und Rüstungskontrolle in der Cyber-Kriegsführung seit 2011 beteiligt (bitte nach Ressorts aufschlüsseln)?

Auswärtiges Amt:

- Gruppe der Regierungssachverständigen der Vereinten Nationen zum Thema internationale Cybersicherheit (GGE) 2012 – 2013, 2014 – 2015 sowie, unter deutschem Vorsitz, 2016 – 2017
- Informelle Arbeitsgruppe Informations- und Kommunikationstechnologie der Organisation für Sicherheit und Zusammenarbeit in Europa
- Internationale Rüstungskontroll-Konferenz „2019. Capturing Technology. Rethinking Arms Control.“ am 15. März 2019 in Berlin

Bundesministerium der Verteidigung:

- GGE der Vereinten Nationen zum Thema internationale Cybersicherheit (unter Federführung des Auswärtigen Amts)
- Informelle Arbeitsgruppe Informations- und Kommunikationstechnologie der Organisation für Sicherheit und Zusammenarbeit in Europa (unter Federführung des Auswärtigen Amts)
- Internationale Rüstungskontroll-Konferenz „2019. Capturing Technology. Rethinking Arms Control.“ am 15. März 2019 in Berlin (unter Federführung des Auswärtigen Amts)

9. Schließt die Bundesregierung

   a) das Vorhandensein von Software-Implantaten anderer Staaten zum Monitoring von Computersystemen (vgl. https://nyti.ms/30BlFmK) in kritischen Infrastrukturen in Deutschland bzw.

Das Vorhandensein von Software-Implantaten in Computersystemen kann für jegliche IT-Infrastruktur durch die Bundesregierung nicht grundsätzlich ausgeschlossen werden.

   b) die Entwicklung oder Beschaffung vergleichbarer Software-Artefakte zur Verwendung in kritischen Infrastrukturen anderer Staaten aus?

Die Bundesregierung schließt aus, Software-Artefakte im Sinne der Fragesteller ohne die entsprechenden, insbesondere völkerrechtlichen, Rechtsgrundlagen einzusetzen.

10. Welche rechtlichen Studien, Einschätzungen und Bewertungen zieht die Bundesregierung für ihre Überlegungen zu Hackback-Maßnahmen und der damit einhergehenden Gefahr einer militärischen Eskalation heran?

Bei der Prüfung der im Zusammenhang mit Maßnahmen der aktiven Cyber-Abwehr aufgeworfenen Fragestellungen setzt sich die Bundesregierung mit einer Vielzahl an Rechtsauffassungen auseinander. Diese gelangen der Bundesregierung in unterschiedlichen Darstellungsformen zur Kenntnis (z. B. in Form von Aufsätzen, Gutachten, Vorträgen, Äußerungen auf Podiumsdiskussionen usw.). Die Bundesregierung führt keine Zusammenstellung aller Rechtsauffassungen, die sie zur Kenntnis nimmt.

11. Teilt die Bundesregierung die Sichtweise der in der Vorbemerkung der Fragesteller genannten NATO-Expertinnen und NATO-Experten, dass durch staatliche Stellen ausgeführte Cyberangriffe eine Form militärischer Angriffe darstellen können, und inwiefern berücksichtigt sie dies bei ihren Überlegungen zu Hackback-Maßnahmen?

Cyberangriffe können einen bewaffneten Angriff im Sinne von Artikel 51 der VN-Charta darstellen. Auf die Antwort zu den Fragen 3 bis 5 wird verwiesen.

12. Erwägt die Bundesregierung Mechanismen zur Bewertung von Eskalationsrisiken von Hackbacks und anderen Cyber-Operationen?

   a) Wenn ja, welche?

      Ist dabei auch eine politische Bewertungsinstanz vorgesehen?

   b) Wenn nein, weshalb nicht?

Die Fragen 12 bis 12b werden zusammen beantwortet.

Der Einsatz militärischer Fähigkeiten im Cyber-Raum erfolgt im Rechtsrahmen, der durch das Grundgesetz und das Völkerrecht gesteckt wird. Die gültigen Prozesse für Operationsplanung und -führung gewährleisten die politische Kontrolle des Einsatzes aller militärischer Fähigkeiten und beinhalten immer auch eine Risikoabschätzung.

Hinsichtlich Maßnahmen der aktiven Cyber-Abwehr wird auf die Antwort zu den Fragen 3 bis 5 verwiesen.

13. Legt die Bundesregierung Datensammlungen zur Analyse der Urheberschaft von Cyber-Angriffen an?

    a) Wenn ja, seit wann und auf welcher Rechtsgrundlage?

    b) Werden diese auch mit anderen Stellen der IT-Sicherheit ausgetauscht?

    c) Wenn ja, mit welchen?

    d) Plant die Bundesregierung die Anlegung von Datensammlungen und Zugängen zu Datenströmen zur Analyse der Urheberschaft von Cyber-Angriffen?

Die Fragen 13 bis 13d werden zusammen beantwortet.

Behörden des Bundes sammeln im Rahmen ihres jeweiligen gesetzlichen Auftrages Daten zur Analyse der Urheberschaft von Cyberangriffen. Hierzu zählen auch Informationen, die Aufschluss über die Ursachen von Cyberangriffen geben können. Rechtsgrundlagen für das Sammeln entsprechender Daten sind § 1 Absatz 2 des Gesetzes über den Bundesnachrichtendienst (BNDG) sowie §§ 2 ff. BNDG, §§ 8 ff. i. V. m. § 3 Absatz 1 des Bundesverfassungsschutzgesetzes (BVerfSchG) und § 483 der Strafprozessordnung (StPO). Die jeweiligen Rechtsgrundlagen wurden zu unterschiedlichen Zeitpunkten vom Gesetzgeber geschaffen. Die zuständigen Bundesbehörden übermitteln die gesammelten Daten im Rahmen der jeweils einschlägigen rechtlichen Regelungen auch an andere Stellen, unter anderem auch an die im Cyber-Abwehrzentrum vertretenen Behörden.

14. Inwiefern ist das CERT der Bundeswehr (CERTBw) von den operativen Teilen der Bundeswehr getrennt, bzw. wie wird diese Trennung aufgehoben?

Im Rahmen der Aufstellung des Organisationsbereiches Cyber- und Informationsraum ist das ehemalige CERTBw mit seinen Funktionalitäten als neues Cyber Security Operation Centre der Bundeswehr (CSOCBw) im Zentrum für Cybersicherheit in der Bundeswehr (ZCSBw) aufgestellt worden. Die Abgrenzung des CSOCBw zum Zentrum Cyber-Operationen (ZCO) ist durch die Organisation in unterschiedlichen Dienststellen klar gegeben. Die beiden Dienststellen unterstehen aufgrund ihrer Aufgaben und Einbindungen in Prozesse zwei verschiedenen Kommandos innerhalb des Organisationsbereichs Cyber- und Informationsraum. Das ZCSBw untersteht dem Kommando Informationstechnik der Bundeswehr, das ZCO dem Kommando Strategische Aufklärung.

15. Inwiefern wird das CERTBw nach Integration in das KdoCIR (https://bit.ly/2QwUGUQ) auch bei unklarer Trennung zwischen offensiven und defensiven Aufgaben im KdoCIR am zivilen CERT-Verbund teilnehmen können?

    Auf welche formale Handlungsgrundlage des CERT-Verbundes wird dabei Bezug genommen?

Auf die Antwort zu Frage 14 wird verwiesen. Das CERTBw nimmt daher am Informationsaustausch in vollem Umfang teil.

16. Inwiefern plant die Bundesregierung, ihre Erkenntnisse aus Cyber-Angriffen auch weiterhin mit dem zivilen CERT-Verbund zu teilen?

Die Bundesregierung sieht keinen Änderungsbedarf an der gängigen Praxis.

17. Welche personellen Ressourcen und Mittel erwägt die Bundesregierung für offensive Cyber-Operationen einzusetzen, und welche Einrichtungen und Kapazitäten bestehen diesbezüglich zum jetzigen Zeitpunkt (bitte nach Behörden bzw. GmbHs etc., z. B. BND – Bundesnachrichtendienst –, BfV – Bundesamt für Verfassungsschutz –, ZITIS – Zentrale Stelle für Informationstechnik im Sicherheitsbereich –, KdoCIR, Agentur für Innovation in der Cybersicherheit, Bundespolizei aufschlüsseln)?

Die Bundesregierung versteht die Fragesteller so, dass sie sich mit dem Begriff „offensive Cyber-Operationen“ sowohl auf Aktivitäten der zivilen aktiven Cyber-Abwehr als auch auf Aktivitäten der Streitkräfte im Rahmen ihrer verfassungsgemäßen Auftragserfüllung zur Wirkung im Cyber-Raum beziehen.

Zur aktiven Cyber-Abwehr wird auf die Antwort zu den Fragen 3 bis 5 verwiesen. Darüber hinaus wird auf die Antwort der Bundesregierung zu Frage 1 der Kleinen Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/2645 verwiesen.

Zur Durchführung von Cyber-Operationen verfügt der militärische Organisationsbereich CIR im Zentrum Cyber-Operationen (ZCO) über personelle Ressourcen und Mittel.

Die weitere Beantwortung der Frage 17 als Verschlusssache (VS) mit dem Geheimhaltungsgrad „VS – Nur für den Dienstgebrauch“ wird im Hinblick auf das Staatswohl als erforderlich erachtet, da sie Details zu der Fähigkeit zur Durchführung von Cyberoperationen enthält und die offene Bekanntgabe von Informationen die Durchführung zukünftiger Operationen gefährden könnte.

Auf die eingestufte Anlage wird verwiesen.*

18. Welche Trainings oder „Cyber- Manöver“ haben das KdoCIR bzw. das Zentrum Cyber-Operationen (ZCO) seit deren Gründung mit privaten Firmen durchgeführt („Zentrum Cyber-Operationen kooperiert erfolgreich mit Firma CGI“, https://cir.bundeswehr.de ohne Datum), und in welchen dieser Veranstaltungen übernahm das ZCO die Rolle des „Red-Teams“?

Neben der einmaligen Kooperation des ZCO mit der Firma CGI gibt es keine weiteren Kooperationen des ZCO mit privaten Firmen. In der angesprochenen einmaligen Kooperation hat ZCO die Rolle des „Red Teams“ übernommen.

19. An welchen Cyberübungen der Europäischen Union oder der NATO hat sich die Bundeswehr seit der Antwort der Bundesregierung auf Bundestagsdrucksache 19/1900 mit „Red-Teams“ beteiligt?

Kräfte des ZCO waren seit der Antwort der Bundesregierung auf Bundesdrucksache 19/1900 (vom 26. April 2018) an der Übung Locked Shields 2019 in der Rolle des „Red Teams“ beteiligt.

* Das Bundesministerium der Verteidigung hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

20. Welche Details kann die Bundesregierung zu der bilateralen Kooperation zwischen dem Allied Command Transformation (ACT) der NATO sowie dem Forschungsinstitut Center for Intelligence and Security Studies (CISS) an der Universität der Bundeswehr München (Schriftliche Frage 114 des Abgeordneten Andrej Hunko auf Bundestagsdrucksache 19/8434) mitteilen, und welche Projekte in den Bereichen strategische Vorausschau, Krisenfrüherkennung bzw. Krisenmonitoring „auch unter Rückgriff auf große Datenmengen“ sind dort geplant?

Die bilaterale Zusammenarbeitsvereinbarung zwischen dem Allied Command for Transformation (ACT) und der Universität der Bundeswehr München (UniBw M) vertreten durch das Center for Intelligence and Security Studies (CISS) wurde im Februar 2019 geschlossen. Diese Kooperation zielt auf den Aufbau einer wissenschaftlichen Methodenkompetenz innerhalb des ACT. Im Mai 2019 hat die Auftaktveranstaltung an der UniBw M stattgefunden. Im Übrigen wird auf die Antwort der Bundesregierung auf die Schriftliche Frage 114 des Abgeordneten Andrej Hunko auf Bundestagsdrucksache 19/8434 verwiesen.

21. Inwiefern ist die konzeptionelle Prüfung der Einrichtung eines „Kompetenzzentrums Krisenfrüherkennung“ bei der Bundeswehr inzwischen abgeschlossen, und welche Details kann die Bundesregierung zu dessen Standort, Zielsetzung und technischer Infrastruktur mitteilen?

    Wer leitet das Zentrum?

Die Prüfung im BMVg in Bezug auf die Einrichtung eines „Kompetenzzentrums Krisenfrüherkennung“ ist noch nicht abgeschlossen.

22. Wann wird entschieden, ob das durch einen Lehrstuhlinhaber für Internationale Politik an der Universität der Bundeswehr München geleitete Pilotprojekt „Metis“ über die Dauer von zwei Jahren fortgeführt und demnach nicht am 1. Dezember 2019 endet (http://gleft.de/2WA), und inwiefern zeichnet sich bereits ab, dass das Projekt als erfolgreich oder erfolglos bewertet wird?

Das Pilotprojekt Metis läuft bis zum 30. November 2019. Gegenwärtig findet die Evaluierung des Pilotprojekts statt. Über eine Verstetigung wird nach Abschluss der Evaluierung entschieden.

23. Welche Ergebnisse kann die Bundesregierung zu Prüfungen des Auswärtigen Amts mitteilen, für seine „strategischen Kommunikationsbedarfe“ die computergestützte Auswertung von sozialen Medien zum Erkennen von deutsche Außenpolitik betreffenden Desinformationen und Kampagnendynamiken in den sozialen Medien zu nutzen, und wie könnte dies technisch umgesetzt werden (Bundestagsdrucksache 19/7604, Antwort zu Frage 15)?

Das Pilotprojekt zu Desinformationen und Kampagnendynamik in den sozialen Medien und deren Auswirkungen auf die strategische Kommunikation des Auswärtigen Amts dauert an. Ergebnisse liegen daher noch nicht vor.

24. Wie will die Bundesregierung den geplanten EU-Ratsschlussfolgerungen nachkommen, wonach die Mitgliedstaaten „als Beitrag zu einem EU-weit gemeinsamen Verständnis der hybriden Bedrohungen auch künftig freiwillig Informationen und bewährte Verfahren“ austauschen sollen (Ratsdokument 9675/19), über welche Kanäle wird dies jetzt schon von der Bundesregierung umgesetzt, und inwiefern ist darin das Bundesministerium der Verteidigung eingebunden?

Der Austausch von Informationen und bewährten Verfahren als Beitrag zu einem EU-weit gemeinsamen Verständnis der hybriden Bedrohungen erfolgt im Rahmen der Treffen der Gruppe der Freunde des Vorsitzes (Umsetzung von Maßnahme 1 des Gemeinsamen Rahmens für die Bekämpfung hybrider Bedrohungen), an denen ein Vertreter der Bundesregierung teilnimmt. Das Bundesministerium der Verteidigung ist hierbei im Rahmen der Ressortabstimmung eingebunden.

25. Inwiefern hat die Bundesregierung in Verhandlungen zur Etablierung des Rahmens „für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten“ („Cyberdiplomatischer Reaktionsrahmen“; Ratsdokument 9916/17 im Rahmen der „Cyber Diplomacy Toolbox“) dafür votiert, Listungen für Sanktion im Mehrheitsverfahren zu beschließen (vgl. Bundestagsdrucksache 19/10273, Frage 8; falls ja, bitte die Gründe darlegen)?

In den Verhandlungen über einen Rahmen für restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen – Verordnung (EU) 2019/796 des Rates vom 17. Mai 2019 und Beschluss (GASP) 2019/797 des Rates – hat sich die Bundesregierung dafür eingesetzt, dass Listungen wie in Artikel 31 Absatz 2 des Vertrags vom 7. Februar 1992 über die Europäische Union vorgesehen mit qualifizierter Mehrheit beschlossen werden sollten. Sie tat dies, um das Verfahren handhabbarer zu machen und den zeitlichen Zusammenhang zwischen dem Handeln böswilliger Akteure und eventueller Sanktionsverhängung zu verkürzen.

26. Enthält der EU-Rahmen zur Beantwortung böswilliger Cyberaktivitäten nach Auslegung der Bundesregierung auch Bestimmungen, die – nach Vorliegen rechtlicher Voraussetzungen – ein Eindringen der Bundeswehr in ausländische staatliche Informationssysteme und das Stören oder Abschalten derselben diplomatisch unterstützen kann?

Der „Cyberdiplomatische Reaktionsrahmen“ und die Umsetzungsleitlinien enthalten keine Bestimmungen, die in die Prärogative der Mitgliedstaaten für ihre nationale Sicherheit eingreifen.

27. Wie viele Mitarbeiterinnen und Mitarbeiter hat das Gemeinsame Lagezentrum Cyber- und Informationsraum (GLZ CIR) bei der Bundeswehr?

Die Beantwortung der Frage 27 als Verschlusssache (VS) mit dem Geheimhaltungsgrad „VS – Nur für den Dienstgebrauch“ wird im Hinblick auf das Staatswohl als erforderlich erachtet, da sie Details zu den Fähigkeiten des KdoCIR enthält und die offene Bekanntgabe von Informationen die Durchführung der Auftragserfüllung zukünftiger Operationen gefährden könnte.

Auf die eingestufte Anlage wird verwiesen.*

---

* Das Bundesministerium der Verteidigung hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

28. Welche Einstufung tragen die Lageberichte der nachgeordneten Bundeswehrdienststellen Kommando Strategische Aufklärung und Zentrum für Operative Kommunikation, die im Rahmen des Projekts „Lagebild für den Cyber- und Informationsraum“ als Datenquellen dienen (Bundestagsdrucksache 19/10391, Antwort zu Frage 3)?

Die Lageberichte der aufgeführten Dienststellen sind, je nach Schutzbedürftigkeit, in einem Spektrum von „VS – Nur für den Dienstgebrauch“ bis „Geheim“ eingestuft.

a) Welche Fachpublikationen werden hierfür ausgewertet, und wer sucht diese aus?

Für die Lageberichte werden durch den jeweiligen Analysten offene Informationsquellen ausgewertet, die im Einzelfall auch themenspezifische Fachpublikationen beinhalten können.

b) Welche Einstufung trägt die aus den verschiedenen Datenquellen erstellte „Lage für den Cyber- und Informationsraum“, die auch an den Militärischen Abschirmdienst und das Nationale Cyber-Abwehrzentrum verteilt wird?

Die "Lage für den Cyber- und Informationsraum" wird, abhängig von der Schutzbedürftigkeit des Inhalts, in einem Spektrum von „VS – Nur für den Dienstgebrauch“ bis „Geheim“ eingestuft.

29. Welche Rolle haben die Cyber-Abwehr und damit verbundene Fragen in der Kooperation mit Frankreich und insbesondere im Rahmen des Aachener Vertrags gespielt, und inwiefern sind zukünftige gemeinsame Projekte dazu vorgesehen?

Im Austausch zwischen dem Bundesministerium des Innern, für Bau und Heimat (BMI) und der französischen Autorité Nationale en matière de Sécurité et de défense des Systèmes d’Information (ANSSI) werden regelmäßig Informationen zu den jeweiligen Planungen im Bereich der Cybersicherheit ausgetauscht. Dazu gehören anlassbezogen auch Fragen der Cyberabwehr. Planungen für konkrete gemeinsame Projekte hierzu existieren nicht.

30. Mit welchen französischen Stellen hat sich die Bundesregierung entsprechend des Artikels 21 des Aachener Vertrags zur Frage ethischer Leitlinien für neue Technologien auf internationaler Ebene ausgetauscht, welche ethischen Fragestellungen und Probleme wurden dabei zugrunde gelegt, welche gemeinsamen Positionen wurden erarbeitet, und auf welchen internationalen Ebenen (UN, OSZE, Europarat, EU und andere) setzen sich Frankreich und Deutschland auf welche Weise für solche ethischen Leitlinien ein?

Die von der Bundesregierung eingesetzte Datenethikkommission (DEK) erarbeitet zurzeit unter anderem Empfehlungen für ethische Leitlinien beim Umgang mit Daten, Algorithmen und Künstlicher Intelligenz (KI). Die DEK wird ihre Empfehlungen am 23. Oktober 2019 vorstellen.

Der Prozess zwischen Deutschland und Frankreich soll auf diesen Empfehlungen aufbauen und in die Diskussion über den Einsatz für ethische Leitlinien für neue Technologien und gemeinsame Werte in den Bereichen Digitalisierung und Digitale Gesellschaft auf EU-Ebene einfließen.

Die Umsetzung des deutsch-französischen Vorhabens wird seitens des Bundesministeriums des Innern, für Bau und Heimat und des Bundesministeriums der Justiz und für Verbraucherschutz vorbereitet.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333